**LISTING OF CLAIMS:**

Claim 1 (cancelled) A remotely accessible secure cryptographic system for storing a plurality of private cryptographic keys to be associated with multiple users, wherein said secure cryptographic system associates each of said multiple users with one or more different keys from said plurality of private cryptographic keys and performs cryptographic functions for each user using the associated one or more different keys without releasing said plurality of private cryptographic keys to said users, said secure cryptographic system comprising:

a depository system having at least one server which stores a plurality of private cryptographic keys and a plurality of enrollment authentication data, wherein each enrollment authentication data identifies one of multiple users and each of said multiple users is associated with one or more different keys from said plurality of private cryptographic keys;

an authentication engine which compares authentication data received by one of said multiple users to enrollment authentication data corresponding to said one of multiple users and received from said depository system, thereby producing an authentication result;

a cryptographic engine which, when said authentication result indicates proper identification of said one of the multiple users, performs cryptographic functions on behalf of the one of said multiple users using the associated one or more different keys received from said depository system;

a transaction engine connected to route data from the multiple users to said depository server system, said authentication engine, and said cryptographic engine; and

wherein said secure cryptographic system is remotely accessible.

Claim 2 (currently amended) A secure cryptographic system, comprising:

a depository system, remote from a user, having at least one server which stores at least one private key and a plurality of enrollment authentication data, wherein each enrollment authentication data identifies one of multiple users;

an authentication engine, remote from said user, which compares authentication data received ~~by~~ from one of said multiple users to enrollment

authentication data corresponding to said one of multiple users and received from said depository system, thereby producing ~~an~~ the final authentication result;

a cryptographic engine, remote from said user, which, when said authentication result indicates proper identification of said one of said multiple users, performs cryptographic functions on behalf of said one of said multiple users using at least ~~said~~ one private key received from said depository system;

a transaction engine connected to route data from said multiple users to said depository server system, said authentication engine, and said cryptographic engine; and

wherein said secure cryptographic system is ~~remotely accessible~~ remote from said user and said user is connected to the system via a communication link.

Claim 3 (currently amended) The secure cryptographic system of Claim 2, wherein said depository system further comprises a plurality of data storage facilities, each data storage facility having at least one server storing a substantially randomized portion of said private key and a substantially randomized portion of said plurality of enrollment authentication data.

Claim 4 (previously presented) The secure cryptographic system of Claim 3, wherein each substantially randomized portion is individually undecipherable.

Claim 5 (previously presented) The secure cryptographic system of Claim 2, wherein said enrollment authentication data includes biometric data.

Claim 6 (previously presented) The secure cryptographic system of Claim 5, wherein said biometric data includes finger print patterns.

Claim 7 (previously presented) The secure cryptographic system of Claim 2, wherein said at least one private key corresponds to said secure cryptographic system.

Claim 8 (previously presented) The secure cryptographic system of Claim 2, wherein said at least one private key corresponds to said one of said multiple users.

Claim 9 (previously presented) The secure cryptographic system of Claim 2, wherein said cryptographic functions comprise one of digital signing, encryption, and decryption.

Claim 10 (currently amended) A method of facilitating cryptographic functions, said method comprising:

associating a user from multiple users with one or more keys from a plurality of private cryptographic keys generated and stored on a remote secure server;

receiving authentication data from said user;

comparing, exclusively on said remote secure server, said authentication data received from said user to authentication data stored on said remote secure server corresponding to said user, thereby verifying the identity of said user; and

utilizing said one or more keys from a plurality of private cryptographic keys to perform cryptographic functions on said remote secure server without releasing said one or more keys from a plurality of private cryptographic keys to said user,

wherein said user is connected to said remote secure server via a communication link.

Claim 11 (previously presented) The method of Claim 10, wherein said authentication data corresponding to said user was acquired prior to the step of receiving authentication data from said user.

Claim 12 (original) The method of Claim 10, further comprising receiving a hash of a message or document.

Claim 13 (previously presented) The method of Claim 12, further comprising archiving said hash

Claim 14 (currently amended) An authentication system for uniquely identifying a user through secure storage of said user's enrollment authentication data, said authentication system comprising:

a plurality of data storage facilities, wherein each data storage facility is remote from said user and includes a computer accessible storage medium which stores one of substantially randomized data portions of ~~at least one piece of enrollment authorization data from~~ enrollment authentication data; and

an authentication engine which communicates with said plurality of data storage facilities and comprises

a data splitting module which operates on said enrollment authentication data to create said substantially randomized data portions ~~from said at least one piece of enrollment authorization data~~,

a data assembling module which processes said substantially randomized data portions from at least two of said data storage facilities to assemble ~~said at least one piece enrollment authorization data from said~~ enrollment authentication data, and

a data comparator module which receives current authentication data from a user and compares the current authentication data with the said assembled enrollment authentication data to determine whether said user has been uniquely identified;

wherein said trust engine comprises an authentication system, and

wherein said trust engine is remote from said user and said user is connected to said trust engine via a communication link.

Claim 15 (previously presented) The authentication system of Claim 14, wherein said substantially randomized data portions are not individually decipherable.

Claim 16 (previously presented) The authentication system of Claim 14, wherein said each data storage facility is logically separated from any other data storage facility.

Claim 17 (previously presented) The authentication system of Claim 14, wherein said each data storage facility is physically separated from any other data storage facility.

Claim 18 (previously presented) The authentication system of Claim 14, further comprising a cryptographic engine which, upon the unique identification of said user by said authentication engine, provides cryptographic functionality to ~~the~~ said user.

Claim 19 (previously presented) The authentication system of Claim 14, wherein said plurality of data storage facilities comprises at least one secure server.

Claim 20 (previously presented) The authentication system of Claim 14, wherein unique identification of said user by said authentication engine provides said user authorization to gain access to or to operate one or more systems.

Claim 21 (previously presented) The authentication system of Claim 20, wherein said one or more systems include one or more electronic devices.

Claim 22 (previously presented) The authentication system of Claim 20, wherein said one or more systems include one or more computer software systems.

Claim 23 (previously presented) The authentication system of Claim 20, wherein said one or more systems include one or more consumer electronics.

Claim 24 (previously presented) The authentication system of Claim 23, wherein said one or more consumer electronics includes a cellular phone.

Claim 25 (previously presented) The authentication system of Claim 20, wherein said one or more systems include one or more cryptographic systems.

Claim 26 (previously presented) The authentication system of Claim 20, wherein said one or more systems include one or more physical locations.

Claim 27 (previously presented) The authentication system of Claim 14, wherein at least one of said data storage facilities stores at least some of sensitive data, wherein said at least one of said data storage facilities serves said sensitive data when said authentication engine indicates that said user has been uniquely identified.

Claim 28 (previously presented) The authentication system of Claim 14, further comprising a data vault which stores sensitive data, wherein said data vault serves said sensitive data when said authentication engine indicates that said user has been uniquely identified.

Claim 29 (previously presented) The authentication system of Claim 14, wherein said authentication system engine outputs an indication of whether said user has been uniquely identified.

Claim 30 (previously presented) A cryptographic system, comprising:

a plurality of data storage facilities remote from a user, wherein each data storage facility includes a computer accessible storage medium which stores ~~one of~~ substantially randomized data portions of at least one private cryptographic key from a plurality of private cryptographic keys; and

a cryptographic engine remote from said user which communicates with said plurality of data storage facilities and comprises:

a data splitting module remote from said user which operates on said private cryptographic keys to create said substantially randomized data portions of at least one private cryptographic key,

a data assembling module remote from said user which processes the substantially randomized data portions from at least two of said data storage facilities to assemble said at least one private cryptographic key from said plurality of private cryptographic keys, and

a cryptographic handling module remote from said user which receives said assembled private cryptographic keys and performs cryptographic functions therewith,

wherein said user is remote from said cryptographic system and is connected to it via a communication link.

Claim 31 (previously presented) The cryptographic system of Claim 30, wherein said substantially randomized data portions are not individually decipherable.

Claim 32 (previously presented) The cryptographic system of Claim 30, wherein said each data storage facility is logically separated from any other data storage facility.

Claim 33 (previously presented) The cryptographic system of Claim 30, wherein said each data storage facility is physically separated from any other data storage facility.

Claim 34 (previously presented) The cryptographic system of Claim 30, further comprising an authentication engine which, before the cryptographic functionality may be employed on behalf of a user, uniquely identifies said user.

Claim 35 (previously presented) The cryptographic system of Claim 30, wherein said plurality of data storage facilities comprises at least one secure server.

Claim 36 (currently amended) A method of storing authentication data in geographically remote secure data storage facilities thereby protecting said authentication data against compromise of any individual data storage facility, said method comprising:

receiving authentication data from a user at a trust engine remote from said user;

splitting authentication data into two or more portions with a data splitting module remote from said user;

combining at said remote trust engine ~~said~~ an authentication data portion with a first substantially random value to form a first combined value;

combining ~~said~~ a second authentication data portion with a second substantially random value to form a second combined value;

creating a first pairing of said first substantially random value with said second combined value;

creating a second pairing of said first substantially random value with said second substantially random value;

storing said first pairing in a first secure data storage facility located on a server remote from said user; and

storing said second pairing in a second secure data storage facility remote from said user and said first secure data storage facility;

wherein said trust engine comprises multiple remote data storage facilities; and

wherein said user is remote from said trust engine and is connected to it via a communication link.

Claim 37 (currently amended) A method of storing authentication data comprising:

~~receiving~~ generating private cryptographic ~~data~~ keys within a remote trust engine;

splitting authentication data into at least two portions with a data splitting module remote from a user;

combining ~~said~~ a first authentication data portion with a first set of bits to form a second set of bits;

combining ~~said~~ a second authentication data portion with a third set of bits to form a fourth set of bits;

creating a first pairing of said first set of bits with said third set of bits;

creating a second pairing of said first set of bits with said fourth set of bits;

storing one of said first and second pairings in a first computer accessible storage medium remote from said user; and

storing the other of said first and second pairings in a second computer accessible storage medium remote from both said user and said first computer accessible storage medium,

wherein said remote trust engine comprises multiple computer accessible storage media; and

wherein said user is remote from said trust engine and is connected to it via a communication link.

Claim 38 (original) The method of Claim 37, wherein at least one of said first and second computer accessible storage mediums comprises at least one server.

Claim 39 (previously presented) The method of Claim 37, wherein said first computer accessible storage medium is geographically remote from said second computer accessible storage medium.

Claim 40 (previously presented) The method of Claim 37, wherein the matching of one of said first and second pairings with one of said first and second computer accessible storage mediums is substantially random.

Claim 41 (previously presented) The method of Claim 37, wherein at least one of said first and third sets of bits are substantially random.

Claim 42 (previously presented) The method of Claim 37, wherein at least one of said first and third sets of bits comprises a bit length equal to a bit length of said authentication data.

Claim 43 (previously presented) The method of Claim 37, wherein both said first and second pairings are needed to reassemble said data.

Claim 44 (previously presented) The method of Claim 37, further comprising:

creating a third pairing of said second set of bits with said third set of bits;

creating a fourth pairing of said second set of bits with said fourth set of bits;

storing one of said third and fourth pairings in a third computer accessible storage medium; and

storing the other of said third and fourth pairings in a fourth computer accessible storage medium.

Claim 45 (currently amended) A method of storing portions of private cryptographic ~~data~~ keys in geographically remote secure data storage facilities thereby protecting said cryptographic data against compromise of any individual data storage facility, said method comprising:

~~receiving~~ generating private cryptographic ~~data~~ keys ~~at~~ within a remote trust engine;

splitting each private cryptographic key into at least two portions with a data splitting module remote from a user;

combining at said remote trust engine ~~said~~ a first private cryptographic key portion with a first substantially random value to form a first combined value;

combining ~~said~~ a second private cryptographic key portion with a second substantially random value to form a second combined value;

creating a first pairing of said first substantially random value with said second combined value;

creating a second pairing of said first substantially random value with said second substantially random value;

storing said first pairing in a first secure data storage facility located on a server remote from said user; and

storing said second pairing in a secure second data storage facility remote from both said user and said first secure data storage facility,

wherein said trust engine comprises multiple remote data storage facilities, and

wherein said user is remote from said remote trust engine and is connected to it via a communication link.

Claim 46 (currently amended) A method of storing cryptographic data comprising:

~~receiving~~ generating private cryptographic ~~data~~ keys within a remote trust engine;

splitting each private cryptographic key into at least two portions with a data splitting module remote from a user;

combining said cryptographic ~~data~~ key portions with a first set of bits to form a second set of bits;

combining said cryptographic ~~data~~ key portions with a third set of bits to form a fourth set of bits;

creating a first pairing of said first set of bits with said third set of bits;

creating a second pairing of said first set of bits with said fourth set of bits;

storing one of said first and second pairings in a first computer accessible storage medium remote from said user; and

storing the other of said first and second pairings in a second computer accessible storage medium remote from both said user and said first computer accessible storage medium,

wherein said remote trust engine comprises multiple computer accessible storage media; and

wherein said user is remote from said remote trust engine and is connected to it via a communication link.

Claim 47 (previously presented) The method of Claim 46, wherein at least one of said first and second computer accessible storage mediums comprises at least one server.

Claim 48 (previously presented) The method of Claim 46, wherein said first computer accessible storage medium is geographically remote from said second computer accessible storage medium.

Claim 49 (previously presented) The method of Claim 46, wherein the matching of one of said first and second pairings with one of said first and second computer accessible storage mediums is substantially random.

Claim 50 (previously presented) The method of Claim 46, wherein at least one of said first and third sets of bits are substantially random.

Claim 51 (previously presented) The method of Claim 46, wherein at least one of said first and third sets of bits comprises a bit length equal to a bit length of said cryptographic data.

Claim 52 (previously presented) The method of Claim 46, wherein both said first and second pairings are needed to reassemble said cryptographic data.

Claim 53 (previously presented) The method of Claim 46, further comprising:

creating a third pairing of said second set of bits with said third set of bits;

creating a fourth pairing of said second set of bits with said fourth set of bits;
storing one of said third and fourth pairings in a third computer accessible storage medium; and
storing the other of said third and fourth pairings in a fourth computer accessible storage medium.

Claim 54 (currently amended) A method of handling sensitive data from a plurality of users in a cryptographic system, wherein said sensitive data exists in a useable form only during actions employing said sensitive data, said method comprising:

receiving in a ~~software module~~ remote data assembling module, a substantially randomized sensitive data portion from a first computer accessible storage medium remote from said users;

receiving in said ~~software module~~ data assembling module, a second substantially randomized data portion from a second computer accessible storage medium remote from both said users and said first computer accessible storage medium,

processing said substantially randomized sensitive data and said substantially randomized data in said ~~software module~~ data assembling module to assemble said sensitive data; and

employing said sensitive data in a software engine, on a remote trust engine comprising an authentication engine and a cryptographic engine, to authenticate exactly one of said plurality of users,

wherein said remote trust engine comprises said data assembling module and a software engine; and

wherein said users are remote from the trust engine and are connected to it via a communication link.

Claim 55 (previously amended) The method of Claim 54, further comprising destroying said sensitive data after completion of said action.

Claim 56 (previously amended) The method of Claim 54, wherein said sensitive data includes one of user biometric data and cryptographic key data.

Claim 57 (previously amended) The method of Claim 54, wherein at least one of said first and second computer accessible storage mediums comprise a secure server.

Claim 58 (previously amended) The method of Claim 54, wherein said software module comprises a data assembling module and said software engine comprises one of an authentication engine and a cryptographic engine.

Claim 59 (currently amended) A secure authentication system, on a remote trust engine, comprising:

a plurality of authentication engines, wherein said authentication engine contains a data assembling module which assembles substantially randomized enrollment authentication data portions, from various data storage facilities, to form the enrollment authentication data which ~~each authentication engine receives substantially randomized data portions of at least one piece of enrollment authentication data, which once assembled are designed to~~ uniquely identify a user to a degree of certainty, wherein each authentication engine receives current authentication data to compare to said enrollment authentication data, and wherein each authentication engine ~~determines~~ generates an authentication result; [and]

a redundancy system which receives said authentication result of at least two of said authentication engines and uses said authentication results to determine[[s]] whether said user has been uniquely identified[[;]] ,

wherein the secure authentication system is part of said remote trust engine; and

wherein said remote trust engine is remote from said user and said user is connected to said trust engine via a communication link.

Claim 60 (previously amended) The secure authentication system of Claim 59, wherein said redundancy system determines whether said user has been uniquely identified by following the majority of said authentication results.

Claim 61 (previously amended) The secure authentication system of Claim 59, wherein said redundancy system determines whether said user has been uniquely identified by requiring said authentication results to be unanimously positive before issuing a positive identification.

Claim 62 (previously amended) The secure authentication system of Claim 59, wherein said redundancy system includes a plurality of redundancy modules, and said secure authentication system further comprises:

a plurality of geographically remote trust engines, each trust engine having one of said plurality of authentication engines and one of said redundancy modules,

wherein the redundancy module for at least one of said plurality of trust engines determines whether said user has been uniquely identified using said authentication results from ones of said authentication engines associated with the other trust engines and without using said authentication results from the at least one trust engine.

Claim 63 (currently amended) The secure authentication system of Claim 62, wherein each of said plurality of trust engines includes a depository having a computer accessible storage medium which stores said ~~a~~ substantially randomized data portions of at least one piece of said enrollment authentication data and wherein each depository forwards said substantially randomized data portions of said enrollment authentication data to said plurality of authentication engines.

Claim 64 (original) The secure authentication system of Claim 62, wherein said determination of whether said user has been uniquely identified corresponds to the one of said redundancy modules to first determine a result.

Claim 65 (currently amended) A trust engine system for facilitating authentication of a user, said trust engine system comprising:

a first trust engine comprising a first depository, remote from a user, wherein said first depository includes a computer accessible storage medium which stores substantially randomized data portions of at least one piece of enrollment authentication data from a plurality of enrollment authentication data corresponding to multiple users;

a second trust engine located at a different geographic location than said first trust engine and comprising:

a second depository having a computer accessible storage medium which stores said substantially randomized data portions of at least one piece of said enrollment authentication data;

an authentication engine communicating with said first and second depositories and which assembles at least two of said substantially randomized data portions of at least one piece of said enrollment authentication data into a usable form; and

a transaction engine communicating with said first and second depositories and said authentication engine,

wherein when said second trust engine is determined to be available to execute a transaction, said transaction engine receives authentication data from a user and forwards a request for a data assembling module to assemble ~~said substantially randomized data portions of at least one piece of~~ said enrollment authentication data from substantially randomized data portions ~~to said first and second depositories~~, and wherein said authentication engine ~~receives~~ compares said authentication data from said user ~~said transaction engine~~ and ~~said substantially randomized data portions of at~~

~~least one piece of said~~ enrollment authentication data assembled from said first and second depositories, and determines an authentication result[[.]],

wherein said first and second trust engines are remote from said user and said user is connected to said trust engines via a communication link.

Claim 66 (previously amended) The trust engine system of Claim 65, wherein said determination of whether said second trust engine is available to execute said transaction includes a determination of whether said second trust engine is within geographic proximity to said user.

Claim 67 (previously amended) The trust engine system of Claim 65, wherein said determination of whether said second trust engine is available to execute said transaction includes a determination of whether said second trust engine is currently servicing a light system load.

Claim 68 (previously amended) The trust engine system of Claim 65, wherein said determination of whether said second trust engine is available to execute said transaction includes a determination of whether said second trust engine is currently scheduled for maintenance.

Claim 69 (previously amended) The trust engine system of Claim 65, wherein said first and second trust engines are determined to be available, and an authentication result for said trust engine system follows said first of said first and second trust engines to produce said authentication result.

Claim 70 (cancelled) A method of handling sensitive data in a cryptographic system, wherein said sensitive data exists in a useable form only during actions employing said sensitive data, said method comprising:

receiving in a software module, substantially randomized sensitive data portions from a first computer accessible storage medium;

receiving in said software module, substantially randomized data portions from a second computer accessible storage medium,

processing said substantially randomized sensitive data portions and said substantially randomized data in said software module to assemble said sensitive data; and

employing said sensitive data in a software engine to perform a cryptographic function.

Claim 71 (cancelled) The method of Claim 70, further comprising destroying said sensitive data after completion of said action.

Claim 72 (cancelled) The method of Claim 70, wherein said sensitive data includes one of user biometric data and cryptographic key data.

Claim 73 (cancelled) The method of Claim 70, wherein at least one of said first and second computer accessible storage mediums comprise a secure server.

Claim 74 (cancelled) The method of Claim 70, wherein said software module comprises a data assembling module and said software engine comprises one of an authentication engine and a cryptographic engine.